

VN-0140US

PATENT APPLICATION

THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Takayuki SATO

Appln. No. 09/682,122

Group Art Unit:

Filed: July 25, 2001

Examiner: Unknown

For: **MULTI-UNIT BUILDING WITH SECURE ENTRY SYSTEM**

SUBMISSION OF PRIORITY DOCUMENT(S)

Commissioner for Patents

Washington, D.C. 20231

Sir,

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
Japan	2001-109776	April 09, 2001

A certified copy of the above-noted application(s) is (are) attached hereto.

Respectfully submitted,

Karan Singh

Registration No. 38698

RYUKA IP LAW FIRM

6th Floor, Toshin Building, 1-24-12,
Shinjuku, Shinjuku-ku, Tokyo, Japan

Telephone: +81-3-5366-7377

Facsimile: +81-3-5366-7288

Date: September | |, 2001



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 4月 9日

出 願 番 号

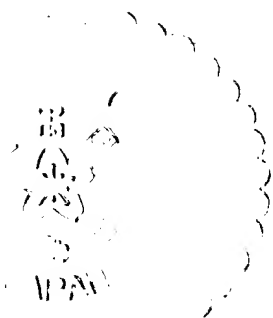
Application Number:

特願2001-109776

出 願 人

Applicant(s):

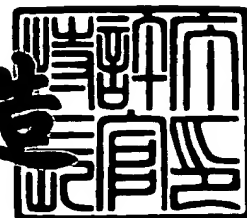
アライドテレシス株式会社



2001年 5月25日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3041839

【書類名】 特許願

【整理番号】 IP214010

【提出日】 平成13年 4月 9日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都品川区西五反田7-22-17 TOCビル ア
ライドテレシス株式会社内

【氏名】 佐藤 貴之

【特許出願人】

【識別番号】 396008347

【氏名又は名称】 アライドテレシス株式会社

【代理人】

【識別番号】 100104156

【弁理士】

【氏名又は名称】 龍華 明裕

【電話番号】 (03)5366-7377

【手数料の表示】

【予納台帳番号】 053394

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 集合建築物

【特許請求の範囲】

【請求項 1】 部内者のみに進入が許容される閉塞空間が複数設けられた集合建築物であって、

当該集合建築物のコンピュータネットワークシステムを統括的に管理する管理サーバと、

前記管理サーバと、前記閉塞空間において使用されるネットワーク機器とを中継する中継機器と

を備え、

前記管理サーバは、前記複数の閉塞空間のそれぞれに対して異なる前記 V L A N を割り当てるべく、前記中継機器を設定することを特徴とする集合建築物。

【請求項 2】 前記閉塞空間への進入しようとする進入者から、当該進入者の識別情報を取得し、前記識別情報に基づいて、前記進入者が前記部内者であるか否かを認証し、前記部内者のみに前記閉塞空間への進入を許容する利用者認証部をさらに備えることを特徴とする請求項 1 に記載の集合建築物。

【請求項 3】 前記管理サーバは、前記閉塞空間の利用者の前記閉塞空間への進入と、前記利用者による前記ネットワーク機器の前記コンピュータネットワークシステムへの進入とを管理することを特徴とする請求項 1 に記載の集合建築物。

【請求項 4】 前記管理サーバは、前記複数の閉塞空間のそれぞれに対して、前記閉塞空間の識別情報である閉塞空間識別情報を割り当て、

前記閉塞空間は、当該閉塞空間に割り当てられた前記閉塞空間識別情報を有する前記利用者の進入を許容することを特徴とする請求項 3 に記載の集合建築物。

【請求項 5】 前記管理サーバは、前記複数の閉塞空間に割り当てられた前記 V L A N のそれぞれに対して、前記 V L A N の識別情報である V L A N 識別情報を割り当て、前記 V L A N に対して割り当てられた前記 V L A N 識別情報を送信した前記ネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項 3 に記載の集合建築物。

【請求項 6】 前記管理サーバは、前記閉塞空間の利用者の前記閉塞空間への進入と、前記利用者による前記ネットワーク機器の前記コンピュータネットワークシステムへの進入との履歴を記憶することを特徴とする請求項 2 に記載の集合建築物。

【請求項 7】 前記管理サーバは、前記複数の閉塞空間のそれぞれに対して、前記管理サーバとは異なる V L A N を割り当てることを特徴とする請求項 1 に記載の集合建築物。

【請求項 8】 前記管理サーバは、前記中継機器に対して、前記管理サーバと同一の前記 V L A N を割り当てることを特徴とする請求項 7 に記載の集合建築物。

【請求項 9】 前記管理サーバは、前記中継機器の接続ポート毎の通信量及び通信時間の少なくとも一方を、前記中継機器から取得し、取得した前記通信量及び前記通信時間の少なくとも一方に基づいて、前記接続ポートの通信を制御することを特徴とする請求項 1 に記載の集合建築物。

【請求項 1 0】 前記閉塞空間において使用される前記ネットワーク機器による前記コンピュータネットワークシステムへの進入を管理するエントランスサーバをさらに備えることを特徴とする請求項 1 に記載の集合建築物。

【請求項 1 1】 前記エントランスサーバは、前記ネットワーク機器の識別情報である機器識別情報を格納するエントランスデータベースを有し、前記エントランスデータベースに格納された前記機器識別情報を有するネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項 1 0 に記載の集合建築物。

【請求項 1 2】 前記エントランスデータベースは、前記機器識別情報として前記ネットワーク機器の M A C アドレスを格納し、

前記エントランスサーバは、前記エントランスデータベースに格納された前記 M A C アドレスを有する前記ネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項 1 1 に記載の集合建築物。

【請求項 1 3】 前記ネットワーク機器の前記 M A C アドレスが、前記エントランスデータベースに格納されていると判断した場合に、当該ネットワーク機

器に対して、IPアドレスを割り当てるDHCPサーバをさらに備えることを特徴とする請求項12に記載の集合建築物。

【請求項14】 前記エントランスサーバは、前記ネットワーク機器の利用者の識別情報である利用者識別情報を格納するエントランスデータベースを有し、前記エントランスデータベースに格納された前記利用者識別情報を送信した前記ネットワーク機器の前記コンピュータネットワークシステムへの進入を許容することを特徴とする請求項10に記載の集合建築物。

【請求項15】 前記管理サーバは、前記エントランスサーバに対して、前記複数の閉塞空間のそれぞれに割り当てられたそれぞれの前記VLANと通信することができるVLANを割り当てることを特徴とする請求項10に記載の集合建築物。

【請求項16】 前記複数の閉塞空間のそれぞれにおいて使用される複数の前記ネットワーク機器に、共通の情報を提供する共用サーバをさらに備えることを特徴とする請求項1に記載の集合建築物。

【請求項17】 前記管理サーバは、前記共用サーバに対して、前記複数の閉塞空間のそれぞれに割り当てられたそれぞれの前記VLANと通信することができるVLANを割り当てることを特徴とする請求項16に記載の集合建築物。

【請求項18】 前記複数の閉塞空間のそれぞれにおいて使用される複数の前記ネットワーク機器のそれぞれにIPアドレスを割り当てるDHCPサーバをさらに備えることを特徴とする請求項1に記載の集合建築物。

【請求項19】 前記管理サーバは、前記DHCPサーバに対して、前記複数の閉塞空間のそれぞれに割り当てられたそれぞれの前記VLANと通信することができるVLANを割り当てることを特徴とする請求項18に記載の集合建築物。

【請求項20】 前記閉塞空間は、前記閉塞空間における異常事態を検出し、前記管理サーバに通知する異常検出手段を有し、

前記異常検出手段は、前記ネットワーク機器が接続される前記中継機器の前記接続ポートの他の接続ポートに接続されることを特徴とする請求項1に記載の集合建築物。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、集合建築物に関する。特に本発明は、管理サーバを備えることにより、セキュリティの高いコンピュータネットワークシステムが形成された集合建築物に関する。

【0002】

【従来の技術】

集合住宅内にルータやハブ等の集線装置を設置することにより、当該集合住宅にLANが構築された集合住宅管理システムが開発されている。従来の集合住宅管理システムでは、インターネットを介して接続された管理サーバによって、集合住宅内に設置された集線装置を管理することにより、住戸間のセキュリティ及びLANの外部に対するセキュリティを管理している。

【0003】

【発明が解決しようとする課題】

しかしながら、従来の集合住宅管理システムでは、インターネットを介して接続された管理サーバによって、集合住宅に構築されたLANを管理するため、LANの外部に対するセキュリティの維持が困難である。また、インターネットを介して接続された管理サーバは、各住戸において使用されるネットワーク機器を詳細に管理をすることが困難である。

【0004】

そこで本発明は、上記の課題を解決することのできる集合建築物を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【0005】

【課題を解決するための手段】

即ち、本発明の第1の形態によると、部内者のみに進入が許容される閉塞空間が複数設けられた集合建築物は、当該集合建築物のコンピュータネットワークシ

システムを統括的に管理する管理サーバと、管理サーバと、閉塞空間において使用されるネットワーク機器とを中継する中継機器とを備え、管理サーバは、複数の閉塞空間のそれぞれに対して異なるVLANを割り当てるべく、中継機器を設定する。

【0006】

閉塞空間への進入しようとする進入者から、当該進入者の識別情報を取得し、識別情報に基づいて、進入者が部内者であるか否かを認証し、部内者のみに前記閉塞空間への進入を許容する利用者認証部をさらに備えてもよい。

【0007】

管理サーバは、閉塞空間の利用者の閉塞空間への進入と、利用者によるネットワーク機器のコンピュータネットワークシステムへの進入とを管理してもよい。管理サーバは、複数の閉塞空間のそれぞれに対して、閉塞空間の識別情報である閉塞空間識別情報を割り当て、閉塞空間は、当該閉塞空間に割り当てられた閉塞空間識別情報を有する利用者の進入を許容してもよい。

【0008】

閉塞空間識別情報は、閉塞空間の出入口に設けられた錠を開閉する鍵の形状であり、錠は、利用者が有する鍵の形状を認証し、閉塞空間は、錠による鍵の形状の認証が成立した場合、利用者の進入を許容してもよい。

【0009】

管理サーバは、複数の閉塞空間に割り当てられたVLANのそれぞれに対して、VLANの識別情報であるVLAN識別情報を割り当て、VLANに対して割り当てられたVLAN識別情報を送信したネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。管理サーバは、閉塞空間の利用者の閉塞空間への進入と、利用者によるネットワーク機器のコンピュータネットワークシステムへの進入との履歴を記憶してもよい。

【0010】

管理サーバは、複数の閉塞空間のそれぞれに対して、管理サーバとは異なるVLANを割り当ててもよい。管理サーバは、中継機器に対して、管理サーバと同一のVLANを割り当ててもよい。

【 0 0 1 1 】

管理サーバは、中継機器の接続ポート毎の通信量及び通信時間の少なくとも一方を、中継機器から取得し、取得した通信量及び通信時間の少なくとも一方に基づいて、接続ポートの通信を制御してもよい。

【 0 0 1 2 】

閉塞空間において使用されるネットワーク機器によるコンピュータネットワークシステムへの進入を管理するエントランスサーバをさらに備えてもよい。エントランスサーバは、ネットワーク機器の識別情報である機器識別情報を格納するエントランスデータベースを有し、エントランスデータベースに格納された機器識別情報を有するネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。

【 0 0 1 3 】

エントランスデータベースは、機器識別情報としてネットワーク機器のMACアドレスを格納し、エントランスサーバは、エントランスデータベースに格納されたMACアドレスを有するネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。ネットワーク機器のMACアドレスが、エントランスデータベースに格納されていると判断した場合に、当該ネットワーク機器に対して、IPアドレスを割り当てるDHCPサーバをさらに備えてもよい。

【 0 0 1 4 】

エントランスサーバは、ネットワーク機器の利用者の識別情報である利用者識別情報を格納するエントランスデータベースを有し、エントランスデータベースに格納された利用者識別情報を送信したネットワーク機器のコンピュータネットワークシステムへの進入を許容してもよい。管理サーバは、エントランスサーバに対して、複数の閉塞空間のそれぞれに割り当てられたそれぞれのVLANと通信することができるVLANを割り当ててもよい。

【 0 0 1 5 】

複数の閉塞空間のそれぞれにおいて使用される複数のネットワーク機器に、共通の情報を提供する共用サーバをさらに備えてもよい。管理サーバは、共用サーバに対して、複数の閉塞空間のそれぞれに割り当てられたそれぞれのVLANと

通信することができるVLANを割り当ててもよい。

【0016】

複数の閉塞空間のそれぞれにおいて使用される複数のネットワーク機器のそれぞれにIPアドレスを割り当てるDHCPサーバをさらに備えてもよい。管理サーバは、DHCPサーバに対して、複数の閉塞空間のそれぞれに割り当てられたそれぞれのVLANと通信することができるVLANを割り当ててもよい。

【0017】

閉塞空間は、閉塞空間における異常事態を検出し、管理サーバに通知する異常検出手段を有し、異常検出手段は、ネットワーク機器が接続される中継機器の接続ポートの他の接続ポートに接続されてもよい。

【0018】

なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【0019】

【発明の実施の形態】

以下、発明の実施形態を通じて本発明を説明するが、実施形態はクレームにかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【0020】

図1は、本発明の一実施形態に係る集合建築物200の構成を示す。本実施形態に係る集合建築物200は、部内者のみに進入が許容される閉塞空間20が複数設けられており、集合建築物200のコンピュータネットワークシステムを統括的に管理する管理サーバ10と、管理サーバ10と閉塞空間20において使用されるネットワーク機器24とを中継する中継機器12とを備える。

【0021】

また、集合建築物200は、集合建築物200のコンピュータネットワークシステムとインターネットとを接続するルータ16をさらに備える。ネットワーク機器24は、ルータ16を介してインターネットを利用することができる。また、インターネット上に設けられた管理装置が、管理サーバ10及び管理データベ

ース14を管理してもよい。

【0022】

管理サーバ10は、複数の閉塞空間20のそれぞれに対して異なるVLANを割り当てべく、中継機器12を設定する。また、閉塞空間20は、当該閉塞空間20に進入する利用者を認証する利用者認証部22を有する。また、閉塞空間20は、ハブ等の集線装置26を有し、閉塞空間20において集線装置26に接続された複数のネットワーク機器24がコンピュータネットワークシステムに接続してもよい。

【0023】

管理サーバ10は、複数の閉塞空間20のそれぞれに対して、閉塞空間20の識別情報である閉塞空間識別情報を割り当てる。また、管理サーバ10は、複数の閉塞空間20のそれぞれに割り当てられたVLANのそれぞれに対して、VLANの識別情報であるVLAN識別情報を割り当てる。そして、管理サーバ10は、複数の閉塞空間20のそれぞれに対応づけて、閉塞空間識別情報及びVLAN識別情報を格納する管理データベース14を有する。

【0024】

管理サーバ10は、閉塞空間20の利用者の閉塞空間20への進入と、利用者によるネットワーク機器24のコンピュータネットワークシステムへの進入とを管理する。閉塞空間20において利用者認証部22は、管理データベース14に基づいて利用者が有する閉塞空間識別情報を認証し、当該閉塞空間20の閉塞空間識別情報を有する利用者の方に当該閉塞空間20への進入を許容する。

【0025】

また、管理サーバ10は、管理データベース14に基づいて閉塞空間20のネットワーク機器24から送信されたVLAN情報識別情報を認証し、当該閉塞空間20に割り当てられたVLANのVLAN識別情報を送信したネットワーク機器24にのみコンピュータネットワークシステムへの進入を許容する。

【0026】

また、管理サーバ10は、閉塞空間20の利用者の当該閉塞空間20への進入と、利用者によるネットワーク機器24のコンピュータネットワークシステムへ

の進入との履歴を記憶してもよい。管理サーバ10は、利用者の当該閉塞空間20への進入と、ネットワーク機器24のコンピュータネットワークシステムへの進入との履歴を記憶することにより、閉塞空間20への不正進入及びコンピュータネットワークシステムへの不正進入を検出することができる。

【0027】

また、閉塞空間20は、当該閉塞空間20において発生した火災、ガス漏れ等の異常事態を検出する異常検出手段を有する。異常検出手段は、中継機器12を介して管理サーバ10に接続され、検出した異常事態を管理サーバ10に通知する。そして、管理サーバ10は、管理者又はセキュリティサービス会社等に通知する。異常事態検出手段は、閉塞空間20のネットワーク機器24が接続される中継機器12の接続ポートと異なる接続ポートに接続されることが好ましい。ネットワーク機器24と異常検出手段とが異なる接続ポートに接続されることによって、ネットワーク機器24の誤作動によって異常検出手段が誤作動することを防止することができる。

【0028】

また、利用者認証部22は、閉塞空間20へ進入しようとする進入者から、当該進入者の識別情報を取得し、識別情報に基づいて、進入者が部内者であるか否かを認証し、部内者のみに閉塞空間20への進入を許容してもよい。また、利用者認証部22は、閉塞空間20の出入口に設けられた錠であってもよく、閉塞空間識別情報は、錠を開閉するための鍵の形状であってもよい。錠は、閉塞空間20の利用者が有する鍵の形状を認証し、錠による鍵の形状の認証が成立した場合、前記利用者の閉塞空間20への進入を許容してもよい。

【0029】

また、管理サーバ10は、例えば管理室などの管理閉塞空間内に配置されてもよい。そして、管理閉塞空間は、当該管理閉塞空間に進入する利用者を認証する利用者認証部を有し、管理サーバ10は、管理データベース14に基づいて、利用者による管理閉塞空間への進入を制限してもよい。

【0030】

本実施形態の集合建築物200によれば、利用者の閉塞空間20への進入を制

限し、さらにネットワーク機器 24 によるコンピュータネットワークへの進入を制限することにより、コンピュータネットワークへの不正な進入に対して高いセキュリティを実現することができる。

【0031】

図 2 は、管理データベース 14 に格納される管理情報ファイルのデータフォーマットを示す。管理情報ファイルは、閉塞空間、閉塞空間識別情報、及び VLAN 識別情報のフィールドを有する。閉塞空間フィールドは、閉塞空間 20 を識別する情報を格納する。閉塞空間識別情報フィールドは、閉塞空間 20 毎に割り当てられ、閉塞空間 20 の利用者を認証するための閉塞空間識別情報を格納する。VLAN 識別情報フィールドは、閉塞空間 20 の VLAN 毎に割り当てられ、VLAN の利用者を認証するための VLAN 識別情報を格納する。管理サーバ 10 は、管理データベース 14 に基づいて、閉塞空間 20 の利用者の閉塞空間 20 への進入と、利用者によるネットワーク機器 24 のコンピュータネットワークシステムへの進入とを管理する。

【0032】

図 3 は、本実施形態に係る集合建築物 200 のコンピュータネットワークシステムの構成を示す。本実施形態に係る集合建築物 200 のコンピュータネットワークシステムは、閉塞空間 20 において使用されるネットワーク機器 24 のコンピュータネットワークへの進入を管理するエントランスサーバ 30 と、複数の閉塞空間 20 において使用される複数のネットワーク機器 24 のそれぞれに IP アドレスを割り当てる DHCP (Dynamic Host Configuration Protocol) サーバ 40 と、複数の閉塞空間 20 のそれぞれにおいて使用される複数のネットワーク機器 24 に共通の情報を提供する共有サーバ 50 とをさらに備える。

【0033】

管理サーバ 10 は、当該管理サーバ 10 に対して、管理 VLAN 100 を割り当てる。また、管理サーバ 10 は、中継機器 12 に対して、当該管理サーバ 10 と同一の管理 VLAN 100 を割り当てる。したがって、管理サーバ 10 は、管理 VLAN 100 において中継機器 12 を制御し、中継機器 12 の接続ポートの

VLAN設定を行うことができる。

【0034】

また、管理サーバ10は、複数の閉塞空間20のネットワーク機器のそれぞれに対して、管理VLAN100とは異なる個別VLAN110a、110b、110c、及び110dを割り当てる。したがって、管理サーバ10は、閉塞空間20において使用されるネットワーク機器24と通信を行うことができない。また、所定の閉塞空間20において使用されるネットワーク機器24は、他の閉塞空間20において使用されるネットワーク機器24と通信を行うことができない。また、管理サーバ10は、エントランスサーバ30、DHCPサーバ40、及び共有サーバ50に対して、複数の閉塞空間20のそれぞれに割り当てられた個別VLAN110a、110b、110c、及び110dと通信することができる全体VLAN120を割り当てる。

【0035】

また、管理サーバ10は、中継機器12の接続ポート毎の通信量及び通信時間の少なくとも一方を、中継機器12から取得する。そして、管理サーバ10は、取得した通信量及び通信時間の少なくとも一方に基づいて、接続ポートの通信を制御する。また、管理サーバ10は、取得した通信量及び通信時間の少なくとも一方に基づいて、課金情報を生成してもよい。管理サーバ10は、中継装置12の接続ポートの通信を制御することによって、当該接続ポートに接続されたネットワーク機器24によるインターネットへの接続等を制限することができる。

【0036】

エントランスサーバ30は、ネットワーク機器24の識別情報である機器識別情報を格納するエントランスデータベース32を有する。エントランスデータベース32は、機器識別情報の一例としてMACアドレスを格納する。エントランスサーバ30は、エントランスデータベース32に格納されたMACアドレスを有するネットワーク機器24のコンピュータネットワークシステムへの進入を許容する。ネットワーク機器24の利用者は、ネットワーク機器24を用いてエントランスサーバ30にログインし、ネットワーク機器24のMACアドレスをエントランスデータベース32に登録する。また、エントランスサーバ30の管理

者が、エントランスサーバ30を用いてネットワーク機器24のMACアドレスをエントランスデータベース32に登録してもよい。

【0037】

また、エントランスデータベース32は、ネットワーク機器24の利用者の識別情報である利用者識別情報を格納してもよい。そして、エントランスサーバ30は、エントランスデータベース32に格納された利用者識別情報に基づいて、ネットワーク機器24から送信された利用者識別情報を認証してもよい。そして、エントランスサーバ30は、利用者の認証が成立した場合に、利用者識別情報を送信したネットワーク機器24のMACアドレスをエントランスデータベース32に格納してもよい。そして、エントランスサーバ30は、利用者識別情報を送信したネットワーク機器24のコンピュータネットワークシステムへの進入を許容してもよい。

【0038】

また、DHCPサーバ40は、エントランスデータベース32に格納されたMACアドレスを有するネットワーク機器24に対して、IPアドレスを割り当ててもよい。DHCPサーバ40が、エントランスデータベース32に登録されたネットワーク機器24のみにIPアドレスを割り当てることによって、登録されたネットワーク機器24のみがインターネットを使用することができる。

【0039】

図4は、エントランスデータベース32に格納されるエントランスファイルのデータフォーマットを示す。エントランスファイルは、閉塞空間、ユーザID、パスワード、及びMACアドレスのフィールドを有する。閉塞空間フィールドは、閉塞空間20を識別する情報を格納する。ユーザIDフィールドは、ネットワーク機器の利用者の識別情報である利用者識別情報を格納する。パスワードフィールドは、利用者識別情報で識別される利用者を認証するためのパスワードを格納する。MACアドレスフィールドは、それぞれの閉塞空間20において使用されるネットワーク機器24のMACアドレスを格納する。

【0040】

ユーザIDフィールドに格納される利用者識別情報、及びパスワードフィール

ドに格納されるパスワードは、ネットワーク機器の利用者又はネットワーク管理者によって予め登録される。そして、MACアドレスフィールドに格納されるMACアドレスは、ネットワーク機器24から受信したMACアドレスが格納される。ネットワーク機器の利用者は、ネットワーク機器を用いてエントランスサーバ30にログインし、ユーザID及びパスワードを入力する。そして、エントランスサーバ30は、入力されたユーザID及びパスワードを、ユーザIDフィールドに格納される利用者識別情報、及びパスワードフィールドに格納されるパスワードによって認証した後、ネットワーク機器24から受信した当該ネットワーク機器のMACアドレスを格納する。

【0041】

また、エントランスデータベース32は、閉塞空間20に対応づけてMACアドレスを格納しており、エントランスサーバ30は、所定の閉塞空間20において、当該所定の閉塞空間20に対応づけて格納されるMACアドレスを有するネットワーク機器24のみにコンピュータネットワークシステムへの進入を許容する。

【0042】

図5は、MACアドレス登録処理のフローチャートを示す。まず、エントランスサーバ30は、中継機器12に接続されたネットワーク機器24のMACアドレスを中継機器12から受信する(S100)。次に、エントランスサーバ30は、エントランスサーバ30にログインしたネットワーク機器24から、当該ネットワーク機器24において利用者によって入力されたユーザID及びパスワードを受信する(S102)。次に、エントランスサーバ30は、エントランスデータベース32を参照し(S104)、受信したユーザID及びパスワードを認証する(S106)。S106において、認証が成立しなかった場合、エントランスサーバ30は、MACアドレスの登録処理を終了する。また、S106において、認証が成立した場合、エントランスサーバ30は、受信したMACアドレスをエントランスデータベース32に登録する(S108)。

【0043】

図6は、MACアドレス照合処理のフローチャートを示す。まず、中継機器1

2は、当該中継機器12に接続されたネットワーク機器24に電源が投入されたことを検知し、エントランスサーバ30に通知する（S200）。次に、エントランスサーバ30は、中継機器12に接続されたネットワーク機器24のMACアドレスを中継機器12から受信する（S202）。次に、エントランスサーバ30は、エントランスデータベース32を参照し（S204）、受信したMACアドレスが格納されているか否かを判断する（S206）。

【0044】

受信したMACアドレスがエントランスデータベース32に格納されている場合、エントランスサーバ30は、DHCPサーバ40に対して、受信したMACアドレスを有するネットワーク機器24へのIPアドレスの割り当てを許可する（S208）。そして、DHCPサーバ40は、エントランスサーバ30の指示に基づいて、ネットワーク機器24にIPアドレスを割り当てる。また、エントランスサーバ30は、中継機器12に対して、受信したMACアドレスを有するネットワーク機器24が接続された中継機器12の接続ポートの通信を許可する（S210）。

【0045】

また、受信したMACアドレスがエントランスデータベース32に格納されていない場合、エントランスサーバ30は、DHCPサーバ40に対して、受信したMACアドレスを有するネットワーク機器24へのIPアドレスの割り当てを禁止する（S212）。また、エントランスサーバ30は、中継機器12に対して、受信したMACアドレスを有するネットワーク機器24が接続された中継機器12の接続ポートの通信を禁止する（S214）。また、エントランスサーバ30は、受信したMACアドレスを有するネットワーク機器24によるコンピュータネットワークシステムへの不正進入であると判断し、受信したMACアドレスを記憶する（S216）。また、エントランスサーバ30は、ネットワーク機器24によるコンピュータネットワークシステムへの不正進入を管理者に通知してもよい。

【0046】

本実施形態の集合建築物200によれば、管理サーバ10、エントランスサー

バ 3 0、D H P C サーバ 4 0、及び共有サーバ 5 0 を備えることにより、中継機器 1 2 及びネットワーク機器 2 4 の詳細な管理を行うことができる。さらに、インターネットを介さずに中継機器 1 2 及びネットワーク機器 2 4 の管理を行うことにより、セキュリティの高いコンピュータネットワークシステムを構築することができる。さらに、登録されたネットワーク機器 2 4 の M A C アドレスに基づいて、コンピュータネットワークシステムを使用できるネットワーク機器 2 4 を制限することにより、コンピュータネットワークシステムへの不正な進入を防ぐことができる。

【 0 0 4 7 】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更または改良を加えることができる。そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【 0 0 4 8 】

【発明の効果】

上記説明から明らかなように、本発明によれば、管理サーバを備えることにより、セキュリティの高いコンピュータネットワークシステムが形成された集合建築物を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る集合建築物 2 0 0 の構成図である。

【図 2】

管理データベース 1 4 に格納される管理情報ファイルのデータフォーマットである。

【図 3】

本実施形態に係る集合建築物 2 0 0 のコンピュータネットワークシステムの構成図である。

【図 4】

エントランスデータベース 3 2 に格納されるエントランスファイルのデータフ

フォーマットである。

【図 5】

MACアドレス登録処理のフローチャートである。

【図 6】

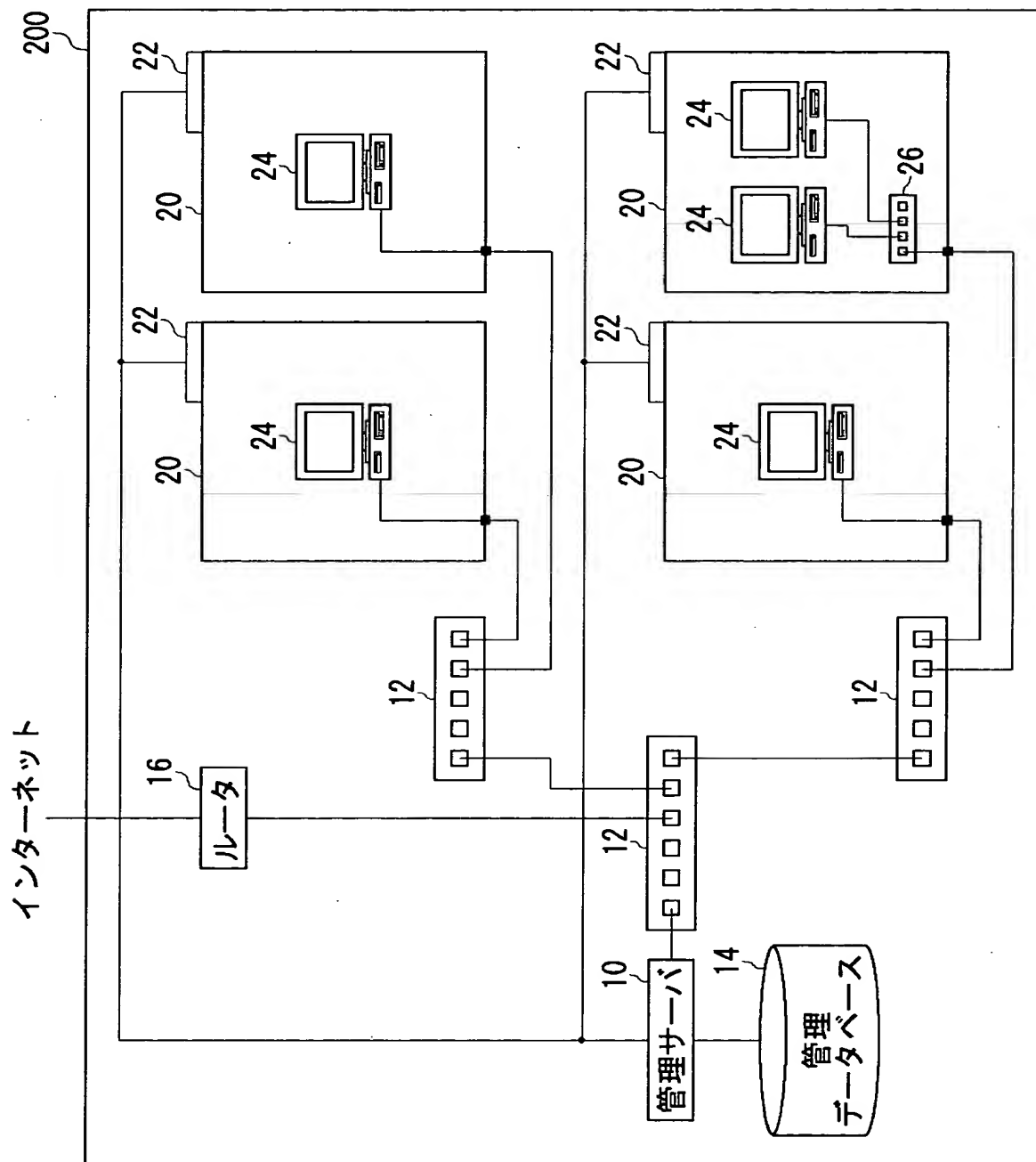
MACアドレス照合処理のフローチャートである。

【符号の説明】

- 10 管理サーバ
- 12 中継機器
- 14 管理データベース
- 16 ルータ
- 20 閉塞空間
- 22 利用者認証部
- 24 ネットワーク機器
- 30 エントランスサーバ
- 32 エントランスデータベース
- 40 DHCPサーバ
- 50 共有サーバ
- 100 管理VLAN
- 110 個別VLAN
- 120 全体VLAN
- 200 集合建築物

【書類名】 図面

【図 1】

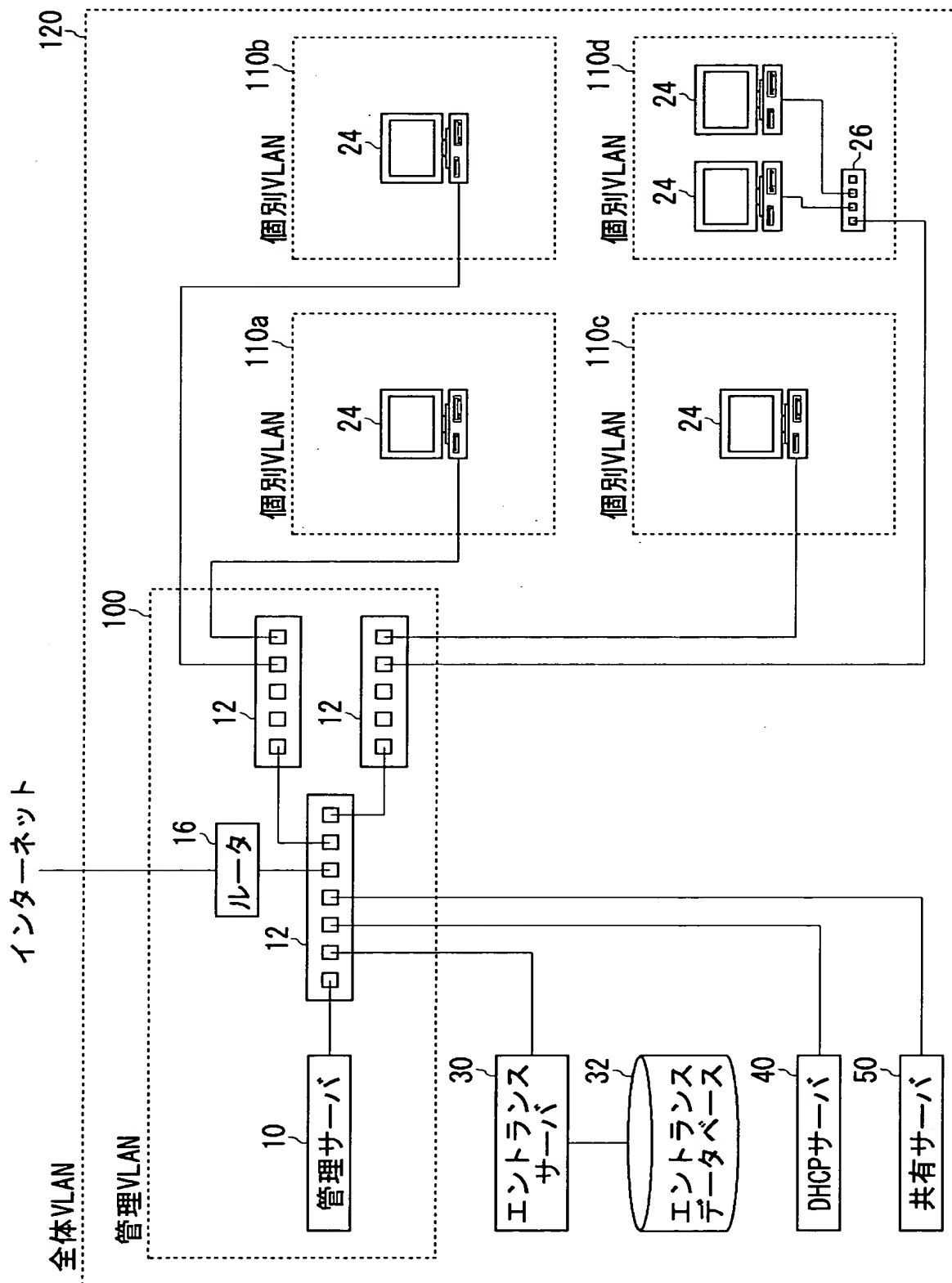


【図 2】

14

閉塞空間	閉塞空間識別情報	VLAN識別情報
101	ABCDE	87326
102	FGHIJ	75981
201	LMNOP	67125
202	QRSTU	66719
⋮	⋮	⋮

【図 3】

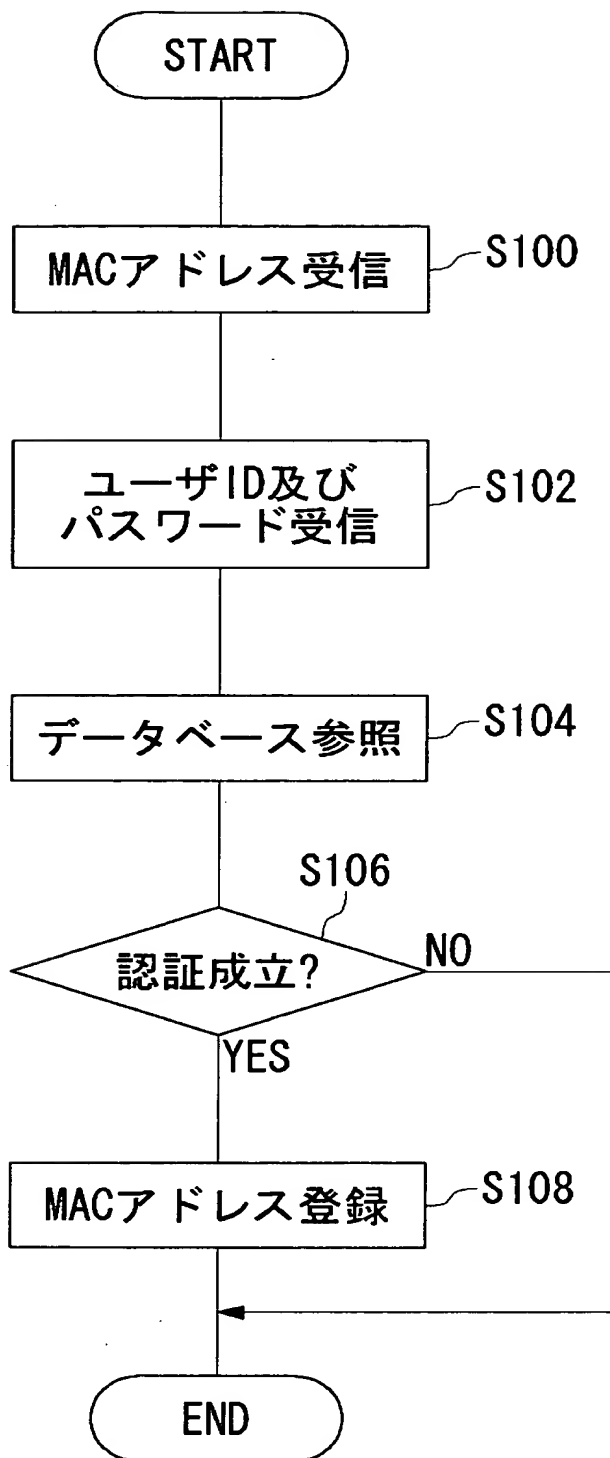


【図 4】

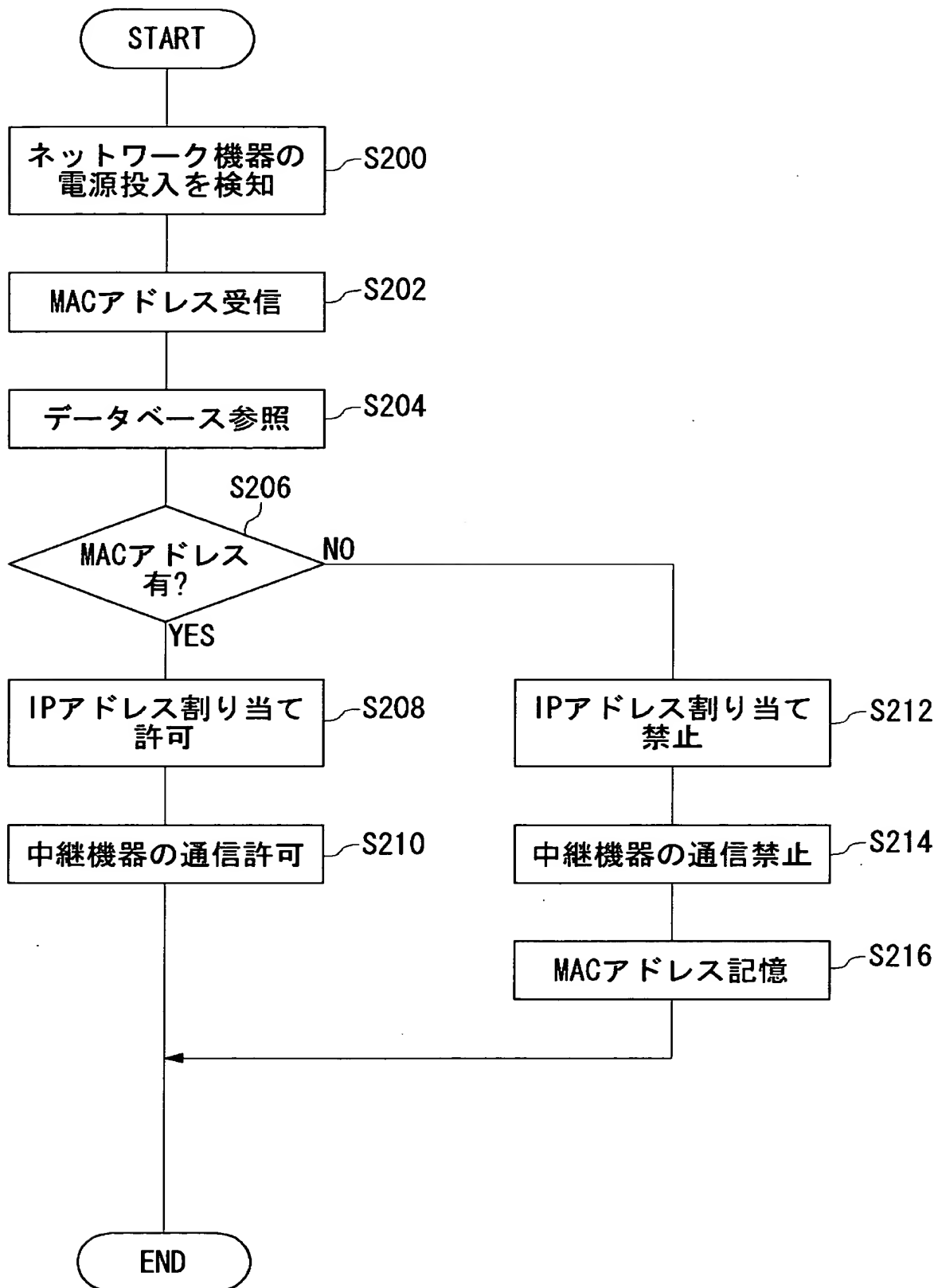
32

閉塞空間	ユーザID	パスワード	MACアドレス
101	aaaaa	*****	50-22-37-AB-66-83
102	bbbbbb	*****	33-51-86-CD-76-10
201	cccccc	*****	55-01-27-EF-60-11
202	ddddd	*****	61-00-10-GF-51-20
	eeee	*****	53-11-02-HI-12-35
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 管理サーバを備えることにより、セキュリティの高いコンピュータネットワークシステムが形成された集合建築物を提供する。

【解決手段】 部内者のみに進入が許容される閉塞空間が複数設けられた集合建築物であって、当該集合建築物のコンピュータネットワークシステムを統括的に管理する管理サーバと、管理サーバと、閉塞空間において使用されるネットワーク機器とを中継する中継機器とを備え、管理サーバは、複数の閉塞空間のそれぞれに対して異なる VLAN を割り当てるべく、中継機器を設定する。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [396008347]

1. 変更年月日 2000年10月24日
[変更理由] 住所変更
住 所 東京都品川区西五反田7-22-17 TOCビル
氏 名 アライドテレシス株式会社